

Configure Windows Vista's firewall

Vista's firewall is more powerful than XP's, but you may need help getting to grips with its extra features, as Jon Thompson explains

You need a firewall built into your PC these days, particularly if you connect using a modem or wireless hot spots. Luckily Windows Vista comes with one built in. It's effective and more powerful than the one that comes with Windows XP, but to access its extra features you must get to grips with an advanced configuration interface.

As far as the casual user is concerned, the XP and Vista versions of Windows Firewall work in a similar way. They both block unwanted connections to your PC from the internet or other network, such as a wireless hotspot. They can also be set up to allow certain incoming connections, which makes it possible to play certain online games.

When a program running on the system receives a connection request from the network, the firewall generates a pop-up window that names the program and asks if you want to keep blocking it, unblock it or defer making a decision. If you choose to unblock the program, the firewall creates an exception and allows the connection. Otherwise, it keeps blocking it.

You can also set exceptions manually for specific ports on which you know you're going to be accepting traffic. For example, if you wanted to run a web server on your PC you'd need to allow incoming traffic on port 80, the default for the HTTP web protocol. If your web server supports encrypted connections over HTTPS, you also need to allow traffic to port 443.

Microsoft's advice on managing exceptions is to keep them to a minimum, which means deleting any you no longer need. It recommends never unblocking programs you don't recognise. So far so good, but Windows XP's firewall has a 'hole'. While it controls traffic coming into the PC from the internet, it does not check traffic being sent from the PC to other

systems. In these days of spyware programs that steal personal details from PCs and send them to computers controlled by criminals, it is important to control data flowing from the PC as well as data entering it.

The Vista version of the firewall takes a different approach to handling traffic. It can filter outgoing connections, but the outgoing filter is disabled by default and requires extra work to get up and running. Once set up, though, it should give you peace of mind that nothing can enter or leave your system without your knowledge and agreement. When used with Windows Defender (see the 'Protect and serve' box opposite), it may be all you need to stay safe online.

NAVIGATING THE FIREWALL

When making the move from XP to Vista, Microsoft shuffled many features around, and many of them have been regrouped. This is frustrating to users who have just upgraded and are learning a new environment. One early review of Vista described it as a jungle.

You'll find the basic Windows Firewall configuration screen by selecting the Security category in the Control Panel and choosing Windows Firewall on the subsequent set of options. As with XP Service Pack 2 (SP2), this screen should indicate that the firewall is up and running by default. If you click the Change Settings link, Vista will ask you explicitly to grant it permission to open the Settings window, which is a tabbed pop-up window similar in appearance to the one in XP.

The General and Exceptions tabs work exactly as they do in Windows XP. On the General tab, you can turn off the firewall. This is not recommended, especially if the machine in question is connected directly to the internet and not protected by a hardware firewall. You can also block all incoming connections.

INTRODUCTION

Vista's firewall comes with some exciting features. On the surface the new firewall looks similar to the old one, but it has powerful hidden depths. Unfortunately, the real gems are quite hard to find.

This month, we show you how to get to grips with the Vista firewall and how to take advantage of the latest security measures.

Jon Thompson
IT Correspondent



contributors@computershopper.co.uk

Vital signs Troubleshooting with ping

Windows contains a handy tool that you can use to find out if other machines on your network are working without having to visit each in person. The ping utility uses the ICMP protocol and can tell you if a machine is reachable (in other words, you can connect to it) and how long it takes to make a connection. Enter this on the command line:

```
ping <IP address or DNS name>
```

To test that your PC can connect to your ADSL router (with the IP address of 192.168.1.1 in this example), simply type:

```
ping 192.168.1.1
```

If this works, you'll want to test that your PC can contact websites. This command can determine whether the PC has access to *Shopper's* website:

```
ping www.computershopper.co.uk
```

It's a good idea to restrict incoming ping requests, as it's a favourite tool for hackers who map networks as a prelude to an attack. You might want to allow a small number of computers to ping yours, but block everyone else. It can be frustrating to find where such restrictions reside in Vista.

Open the Windows Firewall's Advanced Security window. Add an inbound rule and make it a custom type and press Next. Select All Programs and press Next again. Then select the ICMPv4 protocol from the protocol pull-down menu and press Customize. Select the 'Echo Request' ICMP type. Click OK, then Next. Add the IP address for the local machine and that of the machines that are allowed to ping it. Press Next again to allow the connection. Another Next button allows you to set the profile to which the rule applies. Leave all the entries you see ticked. Name the rule and then press Finish.

Using ping from a machine with an IP address other than those on the rule's incoming list will result in a Host Unreachable message.

If you click on the Exceptions tab you'll see some well-known programs have exceptions set for the sake of convenience, including AOL and MSN Messenger. However, these aren't ticked, which means they're still being blocked until you accept connections via a pop-up prompt.

You can also add exceptions by hand here, specific to a program or a port.

ADDING EXCEPTIONS

To add an exception, press the Add Program button. A window pops up listing all installed applications, which it reads from the Windows Registry. Select one of these and press the Change Scope button.

A second window will appear, allowing you to specify which computers can connect to the program you have selected. You can set this to allow any computer, only other computers on your network subnet, or specific IP addresses. Click OK on this and on the program list window and the application you selected will appear in the Exceptions list. Adding an exception rule like this immediately enables it.

You can also create an exception by specifying the port to use. This option is included for expert users. To allow traffic in this way, first press the Add Port button. The resultant pop-up window asks you for the name of the port you want to unblock, its number and whether it's a TCP or UDP port. For safety, you can set the scope of the connections the port can accept here, just as you can for a program.

You can also add exceptions for executables that don't appear on the installed programs list. The Exceptions tab provides the Add Program button, which allows you to enter the path to the program executable. As with the other options, you can change the scope of the connections the program can accept. The Delete button allows you to delete existing exceptions from the list once you no longer need them.

ADVANCED SECURITY

The big difference between the XP and Vista firewalls becomes apparent when you click on the Advanced tab. With Vista, this allows you to control only which network interfaces the firewall should protect, and to restore the factory settings. One positive side-effect of this is that you can see and control the firewall protection on multiple interfaces at once.

If you are looking for other functions that were in the Windows XP firewall, such as logging, bear in mind that Microsoft has hidden these features away. To find them, open the Control Panel and click on System and Maintenance. On the subsequent window, scroll down to the



▲ If you configure your machine's response to the ICMP protocol you could prevent a hacker profiling the machines on your network

Protect and serve Using Windows Defender

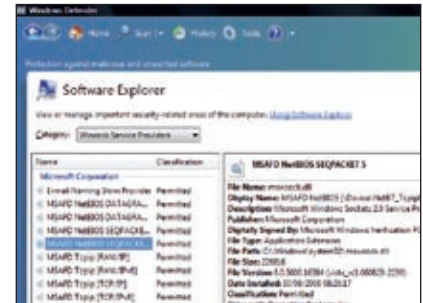
Vista contains a combined anti-virus and anti-spyware system in the form of Windows Defender. Microsoft groups both types of malware into "malicious and unwanted".

Even if you have your own preferred anti-virus and anti-spyware software, you should be able to run Defender, although you may experience some performance issues. If you choose this belt-and-braces approach, open the Control Panel and select the Security section. This should reveal an entry called Windows Defender. Select the Tools icon at the top of the Defender window, then choose Options. You can tell Defender to scan your system at an appropriate time.

Make sure that real-time protection is also enabled. This will scan any program as it loads and runs. Updates to Defender's malware database happen automatically, so you shouldn't be left unprotected.

Defender has a facility called Software Explorer, available from the Tools menu. This lets you view programs in four categories:

those that run at system startup, currently running applications, network connected programs and Winsock service providers. The latter category contains Windows networking services. Clicking on one of the programs in a category will give you far more information than if you'd used Task Manager to inspect it.



▲ Windows Defender's Software Explorer can give you more information about running applications than the Task Manager

Administrative Tools icon at the bottom and click it. This opens a second window, which contains a list of administrative areas in the main pane. The last is Windows Firewall with Advanced Security. Double-click on this. After confirming that you want to continue, the firewall's Advanced Controls window appears.

By clicking on sections of the left-hand pane you can see a general overview of the firewall, any inbound and outbound traffic rules, the rules about who and what can make connections to the machine and the firewall's monitoring options. The central pane displays details of the selected section. The right-hand pane is a context menu, showing the actions you can take.

Click on Windows Firewall with Advanced Security on Local Computer in the left-hand pane. Vista assumes you want to connect to a public network such as the internet, so the public profile is active by default. This is fine, unless you take your Vista laptop computer to work and connect to the corporate network.

BLOCKING THE EXITS

In the middle pane, click the link marked Windows Firewall Properties in the public profile section. A pop-up configuration window lets you turn the firewall on and off, and block not only all inbound traffic but outbound, too, which you can't do in the basic configuration window.

If you block all outbound traffic, you'll stop viruses and spam engines phoning home, but you'll block everything else that doesn't have an exception. Curiously, although the firewall is touted as now being able to prevent outgoing connections, the default is to allow them.

If you block all outgoing connections and then run a program that requires internet access (and which doesn't have an exception), you will receive a pop-up window asking if you want to continue blocking or allow the program access. You will also see this prompt if spyware attempts to connect to the internet. In that case, you'd choose to block its attempt.

The Customize button in the Settings section allows you to switch your blocking notifications on and off for certain programs. This is useful if you're setting up a Vista installation for someone

who may not understand how to deal with the pop-ups that appear. Simply run the programs you know the person will need and create exceptions from the resultant pop-ups.

You'll also find the firewall's logging controls here. Click this section's Customise button and you'll find all the options you may be familiar with from Windows XP. Of these, probably the most important is the default location for the log file, which is buried away in C:\Windows\System32\LogFiles\Firewall\pfirewall.log.

MAKING THE RULES

Rules allow you to take detailed control of how connections will work through your firewall. Add rules using the Windows Firewall With Advanced Security window. For example, first click Inbound Rules in the left-hand pane. Then click New Rule in the right-hand pane. The resulting window lets you apply the rule to all programs or a specific one. If you select the option for a single program, also enter the path to its executable.

Press Next and you can decide whether to allow all incoming connections, allow them only if they are secure or block them. 'Secure' in this context simply means that both ends of the connection will negotiate a suitable level of encryption before data transmission begins. Usually you'll simply allow or block incoming connections to the program. Hitting Next again lets you specify to which profile the rule applies. Leave this screen as it is, hit Next again, name the rule and press Finish.

Expert users can also set up a rule to allow or deny connections to and from individual ports using this method. The only difference is that you enter a port number instead of the path to an executable.

Although the Vista firewall can block outgoing connections, it allows them by default, which is bound to lead to accusations of leaving the PC insecure. Hiding away the ability to enable this feature will likely compound that view in the minds of many. That's unfortunate, because a correctly configured Vista firewall can keep your PC safe while online when used in conjunction with properly configured anti-virus and anti-malware software. **CS**